International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 02 February 2024
Page No: 80 - 86
https://irjaeh.com

A Survey Study on IoT Application and its Attacks

Mashiya Afroze F[1], Dr. Jose Reena K[2]*

[1] Research Scholar, School of Computing Science, Vels Institute of Science, Technology & Advanced Studies, Chennai, India

[2]Assistant Professor, Research Supervisor, School of Computing Science, Vels Institute of Science, Technology & Advanced Studies, Chennai, India

***Emails:** masiamohsin@gmail.com[1], Josereena.scs@velsuniv.ac.in[2]*

*[*]**Orchid ID:** https://orcid.org/0009-0003-4922-4435*

Abstract

The Internet of Things (IoT) has witnessed exponential growth in recent years, with billions of interconnected devices seamlessly communicating and exchanging data. While IoT offers unprecedented opportunities for innovation and convenience, it also introduces a plethora of security challenges. This abstract provides an overview of the key security concerns in IoT and explores emerging solutions to address them. Security in IoT is paramount due to the potential consequences of breaches. IoT devices are often resource-constrained and lack robust security features. Malicious actors can exploit this vulnerability to gain unauthorized access, compromise privacy, launch cyberattacks, and disrupt critical services. Therefore, securing IoT ecosystems is imperative for the continued growth and adoption of IoT technologies.

Keywords: *IoT Internet of Things, IoT application, IoT attacks, Security*

1. Introduction

The Internet of Things (IoT) represents the next communication phase, enabling physical objects to seamlessly generate, transmit, and exchange data. Numerous IoT applications aim to automate various tasks, empowering inanimate objects to function autonomously [1-6]. These applications, both current and forthcoming, hold significant promise in enhancing user comfort, efficiency, and automation. However, realizing this vision on a large scale necessitates robust security measures, encompassing aspects such as privacy, authentication, and resilience against cyberattacks. Consequently, adapting the architecture of IoT applications is crucial to establishing secure end-to-end IoT environments. This paper explores security challenges and potential threats in IoT applications [7-9]. Following the discussion on security issues, the paper examines emerging and established technologies geared towards fostering trust in IoT applications. Specifically, it delves into four key technologies—blockchain, fog computing, edge computing, and machine learning—that play pivotal roles in enhancing IoT security [10].

2. Security Application Areas of IoT

2.1 Smart Home Automation

Remote control of smart thermostats, lighting systems, and appliances enhances energy efficiency and convenience. IoT-enabled home security systems provide real-time monitoring and alerts [11-14].

2.2 Healthcare

IoT-enabled medical devices, such as wearable fitness trackers and insulin pumps, enable remote health monitoring and management, facilitating long-distance patient care [15].

2.3 Smart Cities

IoT-based smart traffic management systems reduce congestion and improve transportation efficiency. Smart street lighting adjusts brightness to save energy, with cloud-based services supporting various smart city applications [16-18].

2.4 Industrial IoT

Predictive maintenance using IoT sensors reduces downtime and costs in industrial machinery.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 02 February 2024
Page No: 80 - 86
https://irjaeh.com

Intelligent environments, like smart airports, utilize IoT technologies for seamless cooperation and dynamic adaptation to changing conditions [19].

2.5 Agriculture

Precision agriculture employs IoT sensors and drones to monitor soil conditions, weather, and crop health, optimizing farming practices and improving crop yields [20-24].

2.6 Retail

IoT systems enable retailers to create digital ecosystems, providing unique offerings and enhancing user experiences through connected, smart systems [25-29].

2.7 Energy Management

IoT platforms support multi-objective energy management systems for renewable energy resources in residential microgrids [30-33]. Hybrid renewable systems integrate multiple energy sources for efficient energy generation [34].

2.8 Environmental Monitoring

IoT sensors monitor humidity, temperature, and air quality for environmental air monitoring, aiding in pollution control and environmental planning [35-39].

2.9 Fleet Management

IoT-based fleet diagnostics systems monitor vehicle conditions and report anomalies, ensuring safe and reliable transportation services [40-42].

2.10 Wearable Technology

Smartwatches, fitness trackers, and other wearable devices collect data on users' health, activity, and location for personal fitness and healthcare [43, 44].

2.11 Supply Chain and Logistics

IoT sensors and RFID tags enable real-time tracking and monitoring of goods during transit, improving supply chain visibility and reducing theft [45-47].

2.12 Building Automation

IoT systems control HVAC systems, lighting, and security in commercial buildings, enhancing energy efficiency and occupant comfort [48-50].

3. Types of attacks on IoT

3.1 Botnets and DDoS Attacks

Botnet attacks initiate with scanning activities and culminate in DDoS attacks, leveraging interconnected IoT devices. The advent of 5G networks introduces new opportunities and challenges for IoT security [51-55].

3.2 Device Spoofing

Attackers impersonate legitimate IoT devices to gain unauthorized access to networks, exploiting vulnerabilities in mobile networks and wireless networks [56-58].

3.3 Eavesdropping (Passive Attacks)

Space/aerial-assisted IoT networks face the risk of eavesdropping attacks, compromising privacy and security. Industrial IoT systems are susceptible to eavesdropping attacks, particularly in highly open transport environments [59-61].

3.4 Man-in-the-Middle (MitM) Attacks

MitM attacks intercept and possibly alter communication between IoT devices, posing threats to network performance and efficiency [62, 63].

3.5 Physical Attacks

Attackers physically tamper with IoT devices to gain access to data or disrupt services [64].

3.6 Malware and Ransomware

Malware infects IoT devices, enabling attackers to gain control and launch ransomware attacks, demanding payment for data decryption [65-67].

3.7 Brute Force Attacks

Attackers attempt to gain unauthorized access to IoT devices by systematically trying different passwords until they find the correct one [68].

3.8 Command Injection

Attackers inject malicious commands into IoT device inputs, exploiting vulnerabilities to gain control over the device [69].

3.9 Firmware and Software Vulnerabilities

Outdated or unpatched firmware and software contain security vulnerabilities that attackers exploit to compromise IoT devices.

3.10 Denial-of-Service (DoS) Attacks

DoS attacks flood IoT devices or networks with excessive traffic, causing device or network overload and service disruption [71].

3.11 Password Attacks

Unauthorized individuals may employ techniques such as dictionary attacks or credential stuffing to

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 02 February 2024
Page No: 80 - 86
https://irjaeh.com

crack passwords and gain illicit access to IoT devices. [69]. Insecure devices exacerbate the magnitude of DDoS attacks, hindering legitimate users' access to critical network services. These vulnerable devices are susceptible to malware, such as backdoors and Trojans, which can infect them and transform them into bots. [72].

Conclusion

This survey addresses numerous security threats across the layers of an IoT application, encompassing the various levels of the IoT architecture. It examines threats targeting the application layer of IoT and discusses different types of attacks that pose risks to IoT systems. By offering insights into these security challenges, this survey aims to provide a valuable reference for enhancing security in future IoT applications.

References

[1]. Sowmik Sarker, Md. Abdur Rakib, Sayemul Islam, Sakib Shahriar Shafin (2022). An IoT-based Smart Grid Technology: Bidirectional Power Flow, Smart Energy Metering, and Home Automation, IEEE 2021 International Conference on Maintenance and Intelligent Asset Management (ICMIAM).

[2]. Shaik Mulla Shabber, Mohan Bansal, P Mrudula Devi, Prateek Jain (2021). iHAS: An Intelligent Home Automation Based System for Smart City, IEEE International Symposium on Smart Electronic Systems (iSES).

[3]. S Imran Hussain; S Deepalakshmi; R J Benilla; V Charu Nivetha, (2023), Automation of Smart Home using Smart Phone via Google Assistant, IEEE 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)

[4]. Souvik Sengupta; Suman Sankar Bhunia (2020), Secure Data Management in Cloudlet Assisted IoT Enabled e-Health Framework in Smart City, IEEE Sensors Journal (Volume: 20, Issue: 16, 15 August 2020)

[5]. Sumedha Nitin Prabhu; Chinthaka P. Gooneratne; Ky-Anh Hoang; Subhas Chandra Mukhopadhyay (2021), IoT-Associated Impedimetric Biosensing for Point-of-Care Monitoring of Kidney Health, IEEE Sensors Journal (Volume: 21, Issue: 13, 01 July 2021) Page(s): 14320 - 14329

[6]. Taiyang Wu, Fan Wu, Chunkai Qiu, Jean-Michel Redouté, and Mehmet Rasit Yuce, (2020), A Rigid-Flex Wearable Health Monitoring Sensor Patch for IoT-Connected Healthcare Applications, IEEE Internet of Things Journal Year: 2020 | Volume: 7, Issue: 8

[7]. Shahid Sultan Hajam; Shabir Ahmad Sofi (2021) IoT-Fog architectures in smart city applications: A survey, China Communications (Volume: 18, Issue: 11, November 2021) Page(s): 117 - 140

[8]. Naman Mishra; Priyank Singhal; Shakti Kundu, (2020) Application of IoT Products in Smart Cities of India, 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)

[9]. Nickolaos Koroniotis; Nour Moustafa; Francesco Schiliro; Praveen Gauravaram; Helge Janicke (2023), The SAir-IIoT Cyber Testbed as a Service: A Novel Cybertwins Architecture in IoT-Based Smart Airports, IEEE Transactions on Intelligent Transportation Systems (Volume: 24, Issue: 2, February 2023) Page(s): 2368 - 2381

[10]. Xiangwang Hou; Zhiyuan Ren; Kun Yang; Chen Chen; Hailin Zhang; Yao Xiao (2019), IIoT-MEC: A Novel Mobile Edge Computing Framework for 5G-enabled IIoT, 2019 IEEE Wireless Communications and Networking Conference (WCNC)

[11]. Abhijeet C. Panchal; Vijay M. Khadse; Parikshit N. Mahalle (2018) Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures, 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)

[12]. Venkata Venugopal Rao Gudlur Saigopal; Valliappan Raju (2020), IIoT Digital Forensics and Major Security issues, 2020 International Conference on Computational Intelligence (ICCI)

[13]. M. Pyingkodi; K. Thenmozhi; K. Nanthini; M.

Karthikeyan; Suresh Palarimath; V. Erajavignesh; G.Bala Ajith Kumar 2022, Sensor Based Smart Agriculture with IoT Technologies: A Review, 2022 International Conference on Computer Communication and Informatics (ICI)

[14]. Jinqi Zhang; Fachuang Zhou; Changrui Jing; Shuangming Wei; Yao Wu; Changrui Jing, Research and Design of Automatic Navigation System for Agricultural Machinery Based on GPS, 2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS)

[15]. Vishesh Garg; Alok Aggarwal; Shalini Aggarwal; Tanishka Bhala; Adarsh Kumar; S.B. Goyal 2022, Multi-utility Agricultural IoT based Robot for Various Agricultural Activities, 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)

[16]. Shailesh O. Kediya; Sanjiv Kumar, 2021, An Analysis of Factors Affecting IoT Adoption by Indian Retail Industry, 2021 International Conference on Computational Intelligence and Computing Applications (ICCICA)

[17]. Sandeep Shekhawat, Use of AI and IoT to make Retail Smarter, 2022 3rd International Informatics and Software Engineering Conference (IISEC)

[18]. Md. Rokonuzzaman; Mahmuda Khatun Mishu; Md. Raishul Islam; Md. Imran Hossain; Mohammad Shakeri; Nowshad Amin, 2021, Design and Implementation of an IoT-Enabled Smart Plug Socket for Home Energy Management, 2021 5th International Conference on Smart Grid and Smart Cities (ICSGSC)

[19]. Sanchit Saxena;Tripti Dhote, 2023, Leveraging IoT Technologies in Retail Industry to improve Customer Experience: Current Applications and Future Potential, 2023 Somaiya International Conference on Technology and Information Management (SICTIM)

[20]. Yajuan Guan; Wei Feng; Yanpeng Wu; Juan C. Vasquez; Josep M. Guerrero, An IoT Platform-based Multi-objective Energy Management System for Residential Microgrids, 2020 IEEE 9th International Power Electronics and Motion Control Conference (IPEMC2020-ECCE Asia)

[21]. Caile Sofia Cabading; John Francis Natividad; Ronald Vincent Santiago, Design of A Hybrid Renewable Energy System with IoT Monitoring and Battery Management, 2022 IEEE 14th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM)

[22]. Dicky Dwi Putra; Budi Syihabuddin; Muhammad Alif Mi'raj Jabbar; Abdurrauf Irsal; Agus Purwadi; Achmad Munir, Energy Management System with IoT Connectivity for Portable Solar Power Plant, 2020 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)

[23]. Zeba Malik; Amit Saxena; Kaptan Singh, Designing a Secure IOT data Encryption algorithm for Smart Environmental Monitoring System, 2021 International Conference on Advances in Technology, Management & Education (ICATME)

[24]. K. Nayanasitachowdary; M. Padmaja, A Real and Accurate GPS based Environmental Monitoring Robotic System using IoT, 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)

[25]. Nwamaka U. Okafor; Declan T. Delaney, Application of Machine Learning Techniques for the Calibration of Low-cost IoT Sensors in Environmental Monitoring Networks, 2020 IEEE 6th World Forum on Internet of Things (WF-IoT)

[26]. M S Punith; M Nithya; K Deepa, IoT Enabled Smart Fleet Management, 2022 IEEE 4th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA)

[27]. Sandip Desai; Ronak Suthar; Vikaskumar Yadav; Vaishnavi Ankar; Vikas Gupta, Smart Bus Fleet Management System Using IoT, 2022 Fourth International Conference on

Emerging Research in Electronics, Computer Science and Technology (ICERECT)
[28]. Jegan Pranav. P; Ancy Jenifer. J; Sweety Janish. A; Narsimha. K; Jeshua Ernest. C, Smart Fleet: An Advanced Web-Based Solution for Fleet Management and Security, 2023 International Conference on Circuit Power and Computing Technologies (ICCPCT)
[29]. Nishank Jain; Alka Chaudhary; Nidhi Sindhwani; Ajay Rana, Applications of Wearable devices in IoT, 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)
[30]. M Rahul Rajesh; B Prashanth Kumar; Ranjeet Kumar; Samineni Peddakrishna; F. John Dian, Study on Recent disputed of Internet of Things (IoT) in Wearable Technologies, 2022 2nd International Conference on Artificial Intelligence and Signal Processing (AISP)
[31]. Haider Raad, A Modular Wearable Technology and IoT Educational Building System Using Brain and Muscular Signals, 2021 Innovation and New Trends in Engineering, Science and Technology Education Conference (IETSEC)
[32]. Mohamed Rawidean Mohd Kassim, Applications of IoT and Blockchain in Smart Agriculture: Architectures and Challenges, 2022 IEEE International Conference on Computing (ICOCO)
[33]. Raad.M. Khaleefah; Nadhim A. M Al-isawi; M. K. Hussein; N.A.M. Alduais, Optimizing IoT Data Transmission in Smart Agriculture: A Comparative Study of Reduction Techniques, 2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)
[34]. Megha Mudholkar; Pankaj Mudholkar; Venkata Harshavardha Reddy Dornadula; K. Sreenivasulu; Kapil Joshi; Bhasker Pant, A Novel Approach to IoT based Plant Health Monitoring System in Smart Agriculture, 2022 5th International Conference on Contemporary Computing and Informatics (IC3I)
[35]. Runxian Tian, Automotive Supply Chain Logistics Management System Based on IOT Technology, 2023 Asia-Europe Conference on Electronics, Data Processing and Informatics (ACEDPI)
[36]. Jin Hou; Cuicui Chen, Intelligent Logistics Supply Chain Management Based on Internet of Things Technology, 2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC)
[37]. Raeesa Bashir; Bhawna Gaur; Arsha Salil, Logistics and IoT Based Survival Strategies to Facilitate Supply Chain Engineering During Pandemic, 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)
[38]. Olivier Debauche; Saïd Mahmoudi; Yahya Moussaoui, Internet of Things Learning a Practical Case for Smart Building automation, 2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech)
[39]. Omar K. T. AL sultan; Abdulbary R. Suleiman, Simulation of IoT Web-based Standard Smart Building Using Packet Tracer, 2021 7th International Engineering Conference "Research & Innovation amid Global Pandemic" (IEC)
[40]. Farhad Muhammed-Ameen Zebari; Mehmet Bilal Er, Power Saving Safety and Remote Controlling Smart Building Based on IoT, 2021 2nd International Informatics and Software Engineering Conference (IISEC)
[41]. F. Hussain et al.: Two-fold Machine Learning Approach to Prevent and Detect IoT Botnet Attacks, 2021. Digital Object Identifier 10.1109/ACCESS.2021.3131014
[42]. KAIFAN HUANG, LU-XING YANG, XIAOFAN YANG 1, YONG XIANG, YUAN YAN TANG, Digital Object Identifier, 10.1109/ACCESS.2020.2977112 A Low-Cost Distributed Denial-of-Service Attack Architecture
[43]. Adam Borys; Abu Kamruzzaman; Hasnain Nizam Thakur; Joseph C. Brickley; Md L. Ali; Kutub Thakur, An Evaluation of IoT DDoS Cryptojacking Malware and Mirai Botnet, 2022 IEEE World AI IoT Congress (AIIoT)

[44]. Manish Snehi; Abhinav Bhandari, Apprehending Mirai Botnet Philosophy and Smart Learning Models for IoT DDoS Detection, 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)
[45]. Hamidreza Ghorbani; M. Saeed Mohammadzadeh; M. Hossein Ahmadzadegan, DDoS Attacks on the IoT network with the emergence of 5G, 2020 International Conference on Technology and Entrepreneurship - Virtual (ICTE-V)
[46]. Cristian Nicolae Capotă; Mădălin Popescu; Simona Halunga; Octavian Fratu, Challenges in Spoofing Bluetooth Low Energy Devices In An IOT Environment, 2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)
[47]. Mohammad Reza Nosouhi; Keshav Sood; Marthie Grobler; Robin Doss, Towards Spoofing Resistant Next Generation IoT Networks, IEEE Transactions on Information Forensics and Security (Volume: 17) Page(s): 1669 – 1683 2022
[48]. Saritakumar N; Anusuya K V; Sreehari Krishnakumar, Detection of ARP Spoofing Attacks in Software Defined Networks, 2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS)
[49]. Jay Thom; Nathan Thom; Shamik Sengupta; Emily Hand, Smart Recon Network Traffic Fingerprinting for IoT Device Identification, 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)
[50]. Mingyuan Liu; Wei Quan; Zhiruo Liu; Yuan Zhang; Deyun Gao; Hongke Zhang, Combating Eavesdropping with Resilient Multipath Transmission for Space/aerial-assisted IoT, ICC 2022 - IEEE International Conference on Communications
[51]. Joseph Henry Anajemba; Celestine Iwendi; Imran Razzak; James Adu Ansere; Izuchukwu Michael Okpalaoguchi, A Counter-Eavesdropping Technique for Optimized Privacy of Wireless Industrial IoT Communications, IEEE Transactions on Industrial Informatics (Volume: 18, Issue: 9, September 2022)
[52]. Abdallah Farraj, Coordinated Security Measures for Industrial IoT Against Eavesdropping, 2023 IEEE Texas Power and Energy Conference (TPEC)
[53]. Gang Liu; Wei Quan; Nan Cheng; Deyun Gao; Ning Lu; Hongke Zhang; Xuemin Shen, Softwarized IoT Network Immunity Against Eavesdropping with Programmable Data Planes, IEEE Internet of Things Journal (Volume: 8, Issue: 8, 15 April 2021) Page(s): 6578 - 6590
[54]. Saritha K; Sarasvathi V; Anvita Singh; Aparna R; Hritik Saxena; Sai Shruthi S, Detection and Mitigation of Man-in-the-Middle Attack in IoT through Alternate Routing, 2022 6th International Conference on Computing Methodologies and Communication (ICCMC)
[55]. Sivasankari N; Kamalakannan S, Fuzzy Logic-based Man-in-the-Middle Attack Detection and Improving Routing Efficiency in the IoT Network, 2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC)
[56]. Ranko Petrović; Dejan Simić; Stefan Stanković; Miroslav Perić, Man-In-The-Middle Attack Based on ARP Spoofing in IoT Educational Platform, 2021 15th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS)
[57]. Devpriya Panda; Brojo Kishore Mishra; Kavita Sharma, A Taxonomy on Man-in-the-Middle Attack in IoT Network, 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)
[58]. Ali Bin Mazhar Sultan; Saqib Mehmood; Hamza Zahid, Man in the Middle Attack Detection for MQTT based IoT devices using different Machine Learning Algorithms, 2022 2nd International Conference on Artificial Intelligence (ICAI)

[59]. Serkan Gönen; Mehmet Ali Barişkan; Derya Yıltaş Kaplan; Ercan Nurcan Yilmaz; Aydın Çetin, A Novel Approach Detection for False Data Injection, and Man in the Middle Attacks in IoT and IIoT, 2023 IEEE PES GTD International Conference and Exposition (GTD)
[60]. Elpida Rouka; Celyn Birkinshaw; Vassilios G. Vassilakis, SDN-based Malware Detection, and Mitigation: The Case of ExPetr Ransomware, 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)
[61]. Muhammad Junaid Iqbal; Sana Aurangzeb; Muhammad Aleem; Gautam Srivastava; Jerry Chun-Wei Lin, RThreatDroid: A Ransomware Detection Approach to Secure IoT Based Healthcare Systems, IEEE Transactions on Network Science and Engineering (Volume: 10, Issue: 5, 01 Sept.-Oct. 2023)
[62]. Hiroki Yasui; Takahiro Inoue; Takayuki Sasaki; Rui Tanabe; Katsunari Yoshioka; Tsutomu Matsumoto, SPOT: Analyzing IoT Ransomware Attacks using Bare Metal NAS Devices, 2022 17th Asia Joint Conference on Information Security (AsiaJCIS)
[63]. Pranshu Bajpai; Richard Enbody, Preparing Smart Cities for Ransomware Attacks, 2020 3rd International Conference on Data Intelligence and Security (ICDIS)
[64]. Yan Jiang; Xiaoyu Ji; Juchuan Zhang; Yancheng Jiang; Shui Jiang; Wenyuan Xu, CapSpeaker: Injecting Commands to Voice Assistants via Capacitors, IEEE Transactions on Dependable and Secure Computing (Early Access) Page(s): 1 – 16, 2023
[65]. Shilpa S Chaudhari; D A Deepthi Yamini, Harris Hawk Optimization-Based Distributed Denial of Service Attack Detection in IoT Networks, 2023 4th International Conference for Emerging Technology (INSET)
[66]. Varalakshmi; M. Thenmozhi; R. Sasi, Detection of Distributed Denial of Service Attack in an Internet of Things Environment - A Review, 2021 International Conference on System, Computation, Automation and Networking (ICSCAN)
[67]. Jared Mathews; Prosenjit Chatterjee; Shankar Banik, CoAP-DoS: An IoT Network Intrusion Data Set, 2022 6th International Conference on Cryptography, Security and Privacy (CSP)
[68]. Huanhuan Lian; Yafang Yang; Yunlei Zhao, Efficient and Strong Symmetric Password Authenticated Key Exchange With Identity Privacy for IoT, IEEE Internet of Things Journal (Volume: 10, Issue: 6, 15 March 2023) Page(s): 4725 – 4734
[69]. Yue Fu; Man, Ho Au; Rong Du; Haibo Hu; Dagang Li, Cloud Password Shield: A Secure Cloud-based Firewall against DDoS on Authentication Servers, 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS)
[70]. Razib Hayat Khan; Jonayet Miah, Performance Evaluation of a new one-time password (OTP) scheme using stochastic petri net (SPN), 2022 IEEE World AI IoT Congress (AIIoT)
[71]. Ramiz Salama; Fadi Al-Turjman; Shruti Bhatla; Satya Prakash Yadav, Social engineering attack types and prevention techniques- A survey, 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN)
[72]. https://www.researchgate.net